IDA

INSTITUTE FOR DEFENSE ANALYSES

Evaluation of DoD Policies for the Release and Distribution of Software

Alfred E. Brenner

September 2001

Approved for public release, unlimited distribution.

IDA Paper P-3652

Log: H 01-001805

This work was conducted under contract DASW01 98 C 0067, Task AK-5-1968 for the Office of the Deputy Under Secretary of Defense (Science and Technology). The publication of this IDA paper does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

INSTITUTE FOR DEFENSE ANALYSES

Evaluation of DoD Policies for the Release and Distribution of Software

Alfred E. Brenner

Preface

This document was prepared by the Institute for Defense Analyses (IDA) under the task order, Evaluation of DoD Policies for the Release and Distribution of Software. It responds to the task objective to analyze the current Office of the Secretary of Defense (OSD) and Service processes and policies related to the release and distribution of software, identify the important issues to be normalized and/or resolved, and to provide recommendations to advance the establishment of meaningful approaches to the control of software.

This study was commissioned by Dr. Dolores Etter, the Deputy Under Secretary of Defense (Science & Technology) (DUSD(S&T)) in January 2001. The author would like to thank Dr. Charles Holland and Mr. John Grosh for their guidance and support throughout the execution of the study. In addition, the author would like to thank all the people and organizations that were interviewed for their cooperation and support in this effort.

This document was reviewed by IDA Research Staff Members: Dr. Richard J. Ivanetich and Mr. Michael S. Nash.

Table of Contents

Executive Summary

Background

Since the beginning of the cold war the U.S. and its allies controlled the export of high performance computers because these leading edge tools represent an important enabling technology for military and national security purposes. Today, with the rapid advancement of information technology it is possible to achieve a very high level of computational performance by networking large numbers of readily available desktop computers, thereby limiting the effectiveness of hardware export control policies.

A study led by the Deputy Under Secretary of Defense (Science and Technology) (DUSD(S&T)) concluded that an alternative, more effective, mechanism is to control software that is considered to be sensitive. In January 2001, the U.S. revised its export control regulations to remove export controls on all computer hardware destined for many countries of the world and relaxed the allowed hardware performance level of exports to most of the rest of the world.

Based on these changes, all federal agencies were directed to increase awareness of the existing strong export controls on critical software within government and industry. They were also directed to identify and invest in additional measures for the protection of critical national security software.

Purpose and Approach of the Study

The DUSD(S&T) tasked the Institute for Defense Analyses (IDA) to analyze the current Office of the Secretary of Defense (OSD) and Service processes and policies related to the release and distribution of software, identify the important issues to be normalized or resolved, and provide recommendations to advance the establishment of meaningful approaches to the control of software.

IDA studied the relevant export control laws, the U.S. government agency regulations for their implementation and a selection of DoD Service and agency policy and guidance documents. How effective these were in implementing the export control legislation for software was analyzed using a representative group of computer software developers, users and managers in DoD.

Interviews with more than fifty people provided insight into the real-world issues involved in the export control of software. Within DoD, the interviews were primarily with the research community involved in the development or use of high performance computing (HPC) software and some of the major shared resource centers (MSRC) directors in the DoD High Performance Computing Modernization Program (HPCMP). Other interviews were with Service security, foreign disclosure and public affairs officers, members of the License Division of the Defense Threat Reduction Agency (DTRA) of the Office of the Deputy Under Secretary of Defense (Technology Security Policy), the Air Force Office of Scientific Research (AFOSR), export control personnel from other U.S. gov-

ernment agencies, academics with involvement with DoD programs, and personnel from industrial firms producing software of interest to DoD.

Legal Basis for Export Control

The two relevant federal laws on export control are the Arms Export Control Act (AECA) and the Export Administration Act of 1979 (EAA). The AECA governs the sale and export of defense articles, services and related technical data, and is implemented by the Department of State under the International Traffic in Arms Regulation (ITAR). The EAA governs the export of dual-use items (i.e., those items that have both military and civilian uses including most unclassified articles and services not covered by the AECA) and is implemented by the Department of Commerce under the Export Administration Regulations (EAR).

Both ITAR and EAR are copious and quite complex. The regulations pertaining to computer equipment are more complex than most other equipment regulations because computers are embedded in almost all modern commercial commodities as well as military equipment and weapons. Computer software which is treated as a subset of "technical data" introduces yet additional complexity. Technical data pertains to all types of civilian and military items, spreading this issue into almost every part of the export control regulations.

Both EAR and ITAR carefully exclude from export control most information that results from fundamental research or that is in the public domain, published, or available to the public, independent of where it was developed. The interpretation of these regulations and definitions, along with the allowed exceptions, leads to important ambiguities, which complicate definitive interpretation of the export control status of an individual software item.

Software at Research Facilities

Every research and development (R&D) laboratory, including the DoD laboratories, uses a wide range of software including operating systems, node and network infrastructure and applications, which encompass the myriad of business, data, and general support tools found on computers in any office and a wide variety of mission specific software. The DoD laboratories develop and use a wide range of science- and engineering-based applications, including general science and engineering applications and more specialized engineering or process-based applications for the design, production, or maintenance of weapons systems.

Acting on the directive to focus on controlling critical software, participants in the HPCMP were asked to provide the export control status of all software developed or used in the program. Approximately 100 software codes under development were examined. In many cases, however, it was unclear how to determine what must be export controlled and what was exempt. The various software developers and users employed a multiplicity of approaches, including consulting with security officers, foreign disclosure officers, public affairs officers, and others at their respective laboratories for assistance in making the export control determination. The resulting decision processes varied widely among the various laboratories and the Services.

Many software status cases were decided without adequate knowledge of the relevant regulations. Nevertheless, there were quite a number of examples of appropriate export control status determinations. The most successful cases were those in which a software scientist or engineer developer took the time to understand the export regulations. IDA investigated a number of examples that illustrate the range of problems encountered by the community in its first attempts at export control determination. These examples illustrate some cases that led to appropriate status determinations and other cases where the status determinations are questionable.

Separately, the HPCMP Office asked the directors of all the HPCMP shared resource centers to describe the processes they used to protect export controlled software and data and to identify knowledgeable export control experts. In some cases, the individual identified as the export control expert was not qualified to make the determination of what software was to be export controlled. In many cases — probably most — there was no office or individual at the facility with the necessary credentials to adequately serve in the role.

Issues in Export Control

To properly adhere to the intent of the export control statutes with respect to technical data and software requires attention to three issues: (1) the proper **determination** of the export control status of the technical data or software, (2) the operational **control** of the digital files containing the software and data and the associated technical literature to support the use of the software, and (3) controlling the **dissemination** of the material to foreign nationals. The determination of the export control status of the technical data and software developed in a program has been the most difficult issue.

Much of the software and associated data in question has legitimate dual-use character, is freely distributed within the larger research community, or is an extension of an already widely distributed code. Often equivalent commercial products are available. In these cases, the decision then rests upon the relative effectiveness of certain key parameters of the software under consideration in comparison to other available software. Two important discriminating factors for code specifically constructed for a military application are whether it has equivalent analogs in civil application or has significant military or intelligence applicability. Other important discriminating issues for control are whether the code is based upon general scientific, mathematical or engineering principles or is in the public domain.

Distinguishing between export controlled and export exempt technical data and software is complex and delicate. Data and software should be evaluated in the total context against the export control regulations. Although there is frequently a large gray area, data in the control regime must be controlled and data in the exempt regime should be exempted. Determination of the export regime in which technical data falls is best made by the scientist or engineer responsible for its existence, in collaboration with his superior and the cognizant export control agent in the organization. It is imperative that the export control agent be knowledgeable of both ITAR and EAR, and has an understanding of the unusual characteristics and special attributes of software, or access to technical support on these matters.

Findings

The information gathered in this study leads to the following findings.

- Both the ITAR and EAR are copious, convoluted, and open to a very wide range of interpretation.
- Service guidance on the export control status determination process and identification of the office(s) with responsibility is inadequate.
- Knowledge of export control regulations and policies by the DoD scientific and engineering community developing or using software varies widely.
- Lack of clearly identified individuals with export control knowledge and designated approval authority leaves software developers without expert assistance to facilitate export control status determinations and to obtain the required approvals.
- There is no generally accepted software development strategy that both advances the research program and addresses export control regulations.
- Although all the resource centers invoke standard operating system or equivalent file access control systems for both data and executable software, there are no clearly defined mechanisms to label restricted files with the type of restriction.

The complexity of the export control regulations, especially with respect to software, the lack of a well-defined, publicized, and supported process for determining the export status of software, and the absence of knowledgeable designated approving authorities, sometimes result in software that is determined to be export controlled that should not be, and vice versa.

An Approach to Export Control Determination

A number of relatively easy actions can be taken to improve the export control determination process, striking a balance between protecting the national security and nurturing R&D. These may be characterized as "process definition" and "product analysis."

Process Definition

The DoD Service laboratories should have a well-defined process for determining the export control status of software and technical data. The responsible authority should be explicitly identified and should be knowledgeable of the relevant export control regulations, especially as they apply to technical data. The export control determination should result from a detailed analysis of the technical and regulatory issues by the principal investigator (PI) (or the PI's supervisor) and the export control authority.

To facilitate this export control determination process requires developing a clear and concise document defining the process and explaining the various technical facets to be considered in the determination—a "cookbook" for export control procedures for DoD software under development or in use. The technical issues included should address not only the collection of appropriate clauses from the regulations themselves, but also a discussion of the nuances of interpretation and a list of the secondary issues that may arise. Options as to how best to satisfy both national security concerns and the continuity of R&D should also be included.

Product Analysis

The very first step in analyzing the appropriateness of controlling export of a software product developed in-house is to realistically assess software equivalent to the code under consideration available in the public domain or for sale by a legitimate commercial firm. Only software that enables better solutions either in time or space domains, performs more effectively, is more user friendly, or is more easily extensible than the open alternative software need be controlled. It is counterproductive to control an application when there is a commercial firm selling an equivalent or better software package in the open market.

In many cases the main issue in determining export control status is not the software itself but the particular data used with the application software to solve a specific (military focused) problem. Such cases require more detailed analysis and an evaluation of several options leading, possibly, to multiple versions of the application software, some export controlled and some exempt, may be appropriate.

Recommendations

- Ensure that a well-defined export control determination process is in place within the Services and agencies and identify the responsible authority.
- Develop a clear and concise source book containing the details of the export control determination process, and provide guidance on how to perform the export control determination analysis on any software or technical data item.
- Have export control determinations made by the Service export control authority or authorized representative working directly with the project PI and in conjunction with the PI's management.
- Require periodic re-evaluations of the export control status of all controlled software.
- Require the HPCMP to strengthen procedures for protecting software that is determined to be export controlled.

1. Introduction

1.1 Background

Since the earliest days of the cold war, the U.S. and its allies have controlled the export of high performance computers to sensitive destinations because these leading edge tools represent an important enabling technology for military purposes. Current procedures for export control are based on the 1979 Export Administration Act (EAA) administered by the Department of Commerce (DOC). With the end of the cold war and the expiration of the EAA in 1995, Congress has debated post-cold war versions of the legislation but so far has been unable to produce updated export control legislation.

Current U.S. policy for export control of high performance computers has two complementary objectives; (a) limit the acquisition of computational capabilities by potential adversaries and countries of proliferation concern, and (b) ensure that U.S. computer industries are competitive in the world market. Defining appropriate legislation and implementing regulations that can fulfill these objectives, over some period of time when both the status of our relationships with other countries and the state of technology are changing rapidly, is difficult.

In the autumn of 2000, Congress did extend the 1979 EAA until August 20, 2001. Also, between 1993 and the end of 2000 the President, by Executive Order, revised upward the export control discriminating level of the performance metric five times based upon the realities of the rapidly increasing performance improvements in computer technology.

Advances in computer technology now enable end users to cluster readily available advanced commodity products into very powerful ad hoc supercomputers, thereby bypassing the government's ability to limit the acquisition of supercomputers to potential adversaries. With this realization, along with concerns about a potential loss of U.S. dominance in the world computing market, threatening U.S. economic security, the Deputy Under Secretary of Defense (Science and Technology) (DUSD(S&T)) was asked to conduct a study to develop alternative strategies for the export control of high performance computers. A major conclusion of this study[1] was that rather than controlling hardware, an alternative, more effective, mechanism is to control software that is considered to be sensitive.

In early January 2001, the President announced the sixth revision since 1993 to U.S. export control regulations. The effect of this revision was to entirely remove export controls on all computer hardware destined for most countries of the world. Modest controls

---

[1] Delores M. Etter, Charles J. Holland, and John Grosh, "Export Control of High-Performance Computing: Analysis and Alternatives," *Computing in Science & Engineering*, Vol. 3, No. 3, May/June 2001, pp. 24-31.

continue for the countries of the former Soviet Union, China, Vietnam, Central Europe, the Middle East, India and Pakistan. A complete embargo continues on computer exports to the identified renegade countries, including Iraq, Iran, Libya, North Korea, Cuba, Sudan and Syria.

With these changes all federal agencies were directed to increase the awareness of their personnel and their contractor personnel of the existing strong export controls on software for national security applications and to identify and invest in additional measures for the protection of critical national security software. In response, the DUSD(S&T) initiated this study and the Principal Deputy Under Secretary of Defense (Acquisition, Technology & Logistics) (PDUSD(AT&L)) established a budget line to support the development of a software protection program.

1.2 Purpose and Scope of the Study

The DUSD(S&T) tasked the Institute for Defense Analyses (IDA) to analyze the current Office of the Secretary of Defense (OSD) and Service processes and policies related to the release and distribution of software, identify the important issues to be normalized or resolved, and to provide recommendations to advance the establishment of meaningful approaches to the control of software. The scope of the study was to:

- Analyze current OSD and Service policies related to the release and distribution of software, documenting inconsistencies and deficiencies in these policies.
- Interview important developers and users of critical Defense-related software to assess the adequacy and impact of the current policies.
- Provide recommendations for improved criteria and guidance for addressing the release and distribution of a wide range of software products addressing the "research product" versus "munitions" issue.
- Provide recommendations for improved software release and distribution policies.

1.3 Study Approach

The approach to this study included an analysis of the relevant export control legislation, the U.S. government agency regulations for their implementation and a selection of DoD Service and agency policy and guidance documents. Analysis of two sets of data from the DoD High Performance Computing Modernization Program (HPCMP) provided insight into the real world issues involved in the export control of software. The data was assembled from two initial calls for information to selected participants in the HPCMP. The first call was to those members of the science and engineering community, who develop and use software, asking them for a formal determination of the export control status of their software. The second call for information was directed at the HPCMP resource center directors asking them to describe their operational procedures in protecting the export controlled data. Finally, IDA interviewed more than fifty people, from DoD and other U.S. government agencies, academia and the private sector. The interviewees are listed in Appendix A.

Within DoD, the focus of the interviews was on the research community involved in the development or use of high performance computing (HPC) software in the HPCMP. Although the HPCMP community represents only a small fraction of the total DoD software developer and user community, they are a coherent group with export control issues representative of much of DoD. Note that any export control software issues arising in DoD acquisition processes, which involve quite different entities and procedures, are outside the scope of this study. Interviewees were selected from those who are developing and/or using advanced research software within the DoD laboratories. Some of the major shared resource centers (MSRC) directors and a number of the Computational Technical Area (CTA) leaders associated with the research programs using the HPCMP facilities were also interviewed. Also interviewed were Service security, foreign disclosure and public affairs officers and, members of the License Division of the Defense Threat Reduction Agency (DTRA) of the Office of the Deputy Under Secretary of Defense (Technology Security Policy), and the Air Force Office of Scientific Research (AFOSR).

A particularly informative set of interviews with participants in the Common High Performance Computing Software Support Initiative (CHSSI) of the HPCMP charted the difficulties some of the DoD community of research scientists and engineers had in responding to the initial request for the export control status of the software they had developed. Additionally, we interviewed people from outside of DoD. These included persons involved in export control matters from other U.S. government agencies including DOC, the Department of Energy (DOE) and the National Aeronautics and Space Agency (NASA), some academics with involvement with DoD programs and a number of industrial firms, both large and small, producing software of interest to DoD.

1.4 Organization of this Report

The remainder of this report is organized as follows:

- Chapter 2 – Basis for Export Control: The two primary relevant federal laws and the derivative implementing regulations are discussed. It focuses on those parts of the regulations pertinent to sensitive but unclassified software and technical data.
- Chapter 3 – Software at Research Facilities: Indicates how software and technical data are developed and used at research facilities. It also recounts some early experiences in determining the export control status of software developed and used at the HPCMP resource centers.
- Chapter 4 – Discussion: Introduces and discusses a number of issues relevant to export control determination and execution.
- Chapter 5 – Findings, Consequences, Approach: Lists and discusses the several findings of the study.
- Chapter 6 – Recommendations: Presents recommendations for facilitating an improved and more effective process for export control determination and suggested approaches for implementation.
- Appendices – Provides supporting information.

2. Basis for Export Control

Export control is a complex process that attempts to limit the export of sensitive items that may be detrimental to the security of the U. S. On the other hand, it also diminishes opportunities for U.S. domestic firms to compete worldwide and it impacts U.S. relationships with other nations of the world. A number of laws, Executive Orders, directives and regulations define U.S. policy governing these matters. These constitute a quite large and diverse set of intertwining and overlapping policy material. Although the basic principles are quite clear, the application of the export control process requires taking cognizance of the particulars of each case, which in practice is frequently very difficult.[2]

For the purposes of this report, focusing primarily on the export control of sensitive but unclassified (SBU) software and related technical information, only a fraction of all the export control laws and regulations need be explored. Consequently this chapter introduces only those items relevant to this issue.

2.1 Federal Laws

There are two relevant federal laws on export control. These are the Arms Export Control Act[3] (AECA) and the Export Administration Act[4] of 1979 (EAA). The AECA governs the sale and export of defense articles, services and related technical data and is the legal basis for most export control issues of interest to this study. The Secretary of State, acting for the President, in consultation with the Secretary of Defense, designates which articles and services are defense articles and services. AECA also requires that a proposed foreign recipient of defense articles and services have agreed to certain conditions. These requirements guarantee that the recipient uses the articles in a manner agreed to, and in a manner that maintains the security of the defense articles and services and provides substantially the same degree of security as the U.S. Government.

The EAA governs the export of dual-use items, i.e., those items that have both military and civilian uses including most unclassified articles and services not covered by the AECA. Defense articles, services and related technical data administered under AECA

---

[2] A valuable reference describing a very wide range of international security issues is the International Programs Security Handbook: (Revised June 2000); February 1995, distributed by the Office of DUSD (Policy Support). Available at http://web2.deskbook.osd.mil/htmlfiles/rlframe/REFLIB_Frame.asp?TOC= /htmlfiles/TOC/033eztoc.htm&Doc=/reflib/ddod/033ez/018/033ez018doc.htm&BMK=C1.

[3] Arms Export Control Act (AECA), Pub. L. 94-329 (1976), (22 U.S.C. 2751), June 30, 1976, as amended.

[4] Export Administration Act of 1979, (EAA), Pub. L. 96-72 (1979), (50 U.S.C. 2401-2420), September 29, 1979, as amended.

are not subject to the EAA (Sec. 734.3). EAA controls exports on the basis of their impact on national security, foreign policy or supply availability. It requires the Secretary of Commerce, in consultation with other government officials, to issue implementing regulations. Most of the goods covered by the EAA are not inherently of a military nature. It is the small number of dual-use items, i.e., those that have both a military and a civilian application, which are of concern in this study. The EAA authorizes the Secretary of Defense, in consultation with the Secretary of Commerce, to identify these dual-use goods and review and control their export for national security reasons. The Departments of State and Defense also must coordinate on the export of certain dual-use goods.

2.2 Export Control Regulations

The AECA and the EAA, assign lead responsibility for implementation to the State and Commerce departments respectively. The International Traffic in Arms Regulations (ITAR)[5] implement Section 38 of the AECA with regard to commercial exports of defense articles and related technical data. The ITAR contains in Part 121 the United States Munitions List (USML), which identifies the defense articles and technical data that are subject to export control. The ITAR also covers the administration of and procedures for requesting an export authorization. The Director of the Office of Defense Trade Controls (ODTC), Department of State, administers the ITAR with the technical assistance of DTRA.

The Export Administration Regulations (EAR)[6] govern the export of most goods that are not inherently of a military nature and thus do not qualify as defense articles. It takes special notice of those civilian goods that can also enhance the military capability of the recipient (i.e., dual-use items). The Commerce Control List (CCL), in Part 774 of the EAR, controls dual-use goods and associated technical data. The EAR, which is issued by the Secretary of Commerce in consultation with the Secretaries of Defense and State, implements the legislation contained in the EAA. The EAR is administered by the Bureau of Export Administration (BXA) of DOC.

Both sets of regulations are copious and quite complex. Those parts of the regulations pertaining to computer equipment are more complex than most other equipment item regulations because computers are embedded in almost all modern commercial commodities and military equipment and weapons, thereby permeating almost every section of the EAR and the ITAR. Furthermore, while what constitutes computer equipment is almost entirely unambiguous, including a measure of the computational power[7] of that computer, the issue of computer software is much less precisely defined. Software itself is considered a subset of technical data. (Section 2.3 provides the ITAR's definition of technical data). Technical data pertains to all types of civilian and military items, spreading this

---

[5] Code of Federal Regulations (CFR), Title 22, Parts 120-130. Available at URL: http://www.pmdtc.org.

[6] Code of Federal Regulations, Title 15, Parts 730-774. Available at URL: http://w3.access.gpo.gov/bxa/ear/ear_data.html.

[7] Although quite controversial in its not necessarily uniform effect on commercial sales, a well-defined metric that is used, the Composite Theoretical Performance (CTP) can be calculated for every computer by a formula contained in the EAR.

issue into almost every part of the export control regulations. Furthermore, unlike computer hardware for which a carefully constructed mathematically rigorous formula defines the computational power of a given hardware configuration, no equivalent precise measure for export control discrimination exists for technical data, including software.

The export regulations for computers and software are particularly hard to definitively interpret because references to them appear in almost every part of the regulations. References to a number of other sections in each section of the regulations as shown in Table 1 for the EAR and in Table 2 for the ITAR give some idea of this complexity. Also, since the focus of each part of the regulations is different, the issues relating to computers and software (technical data) frequently appears to be less than fully coherent. Indeed, current Congressional interest in generating a new and revised export control act to replace the soon-to-expire extension of the EAA is driven by a desire to both modernize and uncomplicate the current regulations.

Table 1. Export Administration Regulations (EAR)

Computer and Technical Data (Including Software) Relevant Sections	
Section 738.2	**Commerce Control List (CCL) Structure** **- CCL includes 10 categories and 5 groups, and 4 country groups**
Section 740.6	**Technology and Software Under Restriction (TSR)** **- References 4 other EAR sections**
Section 740.7	**Computers (CTP)** **- References 17 other EAR sections**
Section 742.12	**High Performance Computers** **- References 32 other EAR sections**
Section 742 Supplement No. 3	**High Performance Computers; Safeguard Conditions and Related Information** **- References 4 other EAR sections**
Section 743.1	**Wassenaar Arrangement** **- References 10 other EAR sections**
Section 774 Supplement Nos. 1 & 2	**Category 4 Computers** **- References 18 other EAR sections**

Yet another complicating factor, particularly relevant to the export of technical data, and therefore also to software, is the issue of "deemed exports." Any software or technology that is subject to export control under the EAR (Sec. 734.2 (b) (3)) that is released to a

foreign national is "deemed to be an export" to the home country of the foreign national. By this definition, export of the software or technical data occurs through:

- Visual inspection of the software code or data;
- Oral exchanges of information in the U.S. or abroad; or
- Technical experience, e.g., hands on execution of the software.

Table 2. International Traffic in Arms Regulations (ITAR)

Computer and Technical Data (Including Software) Relevant Sections	
Part 120	**Purpose and Definitions** **- Especially sections 120.1 through 120.17**
Part 121	**The United States Munitions List** **- Multiple (secondary) references to information in twenty-one categories; Some at variance with information in Part 125**
Part 125	**Licenses for the Export of Technical Data and Classified Defense Articles**

However, both the EAR and the ITAR carefully exclude from export control most information qualifying as results of fundamental research or that information that is in the public domain, published, or available to the public, independent of where it was developed. In the case of research performed at or funded by a federal agency the designation authority of information falling into this category is assigned to the federal agency "within any appropriate system devised by the agency" under the EAR and to the authority that approves the public release of technical data under the ITAR.

2.3 Technical Data and Software

Although both sets of regulations pertain to sensitive but unclassified data and software, the ITAR regulations take precedence over the EAR regulations on export control of defense articles and services. Since most technical data and software issues within DoD have some involvement with military equipment or weapons, most DoD export control issues are determined on the basis of the ITAR rather than the EAR regulations.

With respect to software relevant issues, the ITAR (Sec. 120.3) authorizes export control of a "defense article (Sec. 120.6) or service (Sec. 120.9)" with respect to technical data (which includes software):

- "Which is specifically designed, developed, configured, adapted, or modified for a military application, and does not have predominant civil applications, and does not have performance equivalent to those of an article or service used for civil applications; or

- Is specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control is necessary."

Technical data is defined as (Sec. 120.10(a)):

- "Information, other than software as defined below, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles."
- "Classified information relating to defense articles and defense services;
- Information covered by an invention secrecy order;
- Software as defined below directly related to defense articles;
- This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities, or information in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles."

Software is defined as (Sec. 121.8(f)):

- "Software includes, but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis, and repair."

The interpretation of these regulations and definitions, along with the implicit allowed exceptions leads to important ambiguities, which complicate definitive interpretation of the export control status of any individual software item. These extracts, which are quotes from the ITAR, give some indication of the possible interpretive difficulties.

3. Software at Research Facilities

3.1 Technical Data and Software Requirements of Research and Development (R&D) Laboratories

Every R&D laboratory, including the DoD laboratories, uses a wide range of software, including operating systems, node and network infrastructure and other infrastructure elements, and applications. The applications themselves range widely and include the myriad of business, data, and general support tools found on computers in any office and a wide variety of mission relevant software.

The DoD laboratories develop and use a wide range of science- and engineering-based applications, including general science and engineering applications as well as more specialized engineering or process-based applications for the design, production, or maintenance of weapons systems. Most of these applications are commercially available or have been developed at universities or are available as freeware on the Internet. However, many are developed or modified at a DoD R&D laboratory, by contractors, or by colleagues at other DoD or other government laboratories. These application programs all require data, including physical, chemical, electrical, and mathematical constants that are typically widely published. For some military-mission-focused problems, additional data, including parameters or physical constants for unusual materials or conditions, or parameters derived by simulation or experiment, may also be required.

Applications are developed at the DoD research laboratories for a number of reasons. These include the unavailability of required software from commercial sources or from other research institutions and the need for improved versions of similar available software, requiring more efficient performance for problems being studied, improved human interface, etc. Other reasons include the lack of knowledge of the availability of alternate software or the extreme cost of such software.

3.2 Initial DoD Experience with Export Control Determination[8]

Following the relaxation of export controls on hardware in January 2001, and the Presidential directive to focus on controlling critical software, the Office of the Director of Defense Research and Engineering (DDR&E) distributed a memorandum in February 2001 to all the CTA leaders in the High Performance Computing Modernization Program requesting the export control status of all software developed, or used by the developers and users in their area of responsibility This served as a test of the status of the export control determination process. In almost all cases, however, it was unclear how to make

[8] Although the DoD research facilities include a wide range of research centers and laboratories, a large fraction of the critical sensitive but unclassified software is developed under the HPCMP. This report focuses on the experiences of participants in that program.

the determination as to what was to be export controlled and what was exempt. With no prior experience in the matter of export control on the part of almost all of the HPCMP community, and only minimal guidance accompanying the request for the information, most participants were at a loss on how to proceed. Consequently, the various software developers and users utilized a multiplicity of approaches taking advantage of the availability of security officers, foreign disclosure officers, public affairs officers, etc., at the laboratory, for assistance in making the export control determination. This resulted in decision processes that varied widely among the various laboratories and the Services.

Separately, the HPCMP Office asked the directors of all the HPCMP resource centers to describe the export control processes in place at each center and to identify knowledgeable export control experts. Most responses focused on the process—not of determining what should be export controlled—but rather how to implement the control process for that software identified as controlled. In some cases this was further complicated by the focus on encryption software, e.g, Kerberos, which until that time had been more tightly controlled than other software. Also, some of the classified resource centers claimed there was no need to be concerned in defining what software was export controlled because the facility was a classified one! Responses from some other facilities, even those that were unclassified, claimed that all their participants held national security clearances and, therefore, it was not necessary to clearly identify what software was to be export controlled and what was to be considered exempt. In yet other centers, the claim was that all software used at the facility was restricted to no foreign (NOFORN) access.

The request to the resource centers for names of knowledgeable export control points of contact (POC) was formulated with helpful suggested pointers to offices outside the resource centers. In the responses from the resource centers, POCs listed include: software developer, facility manager, network security officer, (information systems) security officer, foreign disclosure officer, science and technology information officer (STINFO), public affairs officer, facility general counsel, and the management above the center. In a number of these cases it is documented that the identified POC was not adequately knowledgeable regarding the determination of what software was to be export controlled. In many cases, there was no office or individual at the facility with the necessary credentials to adequately serve in the POC role.

These requests to the community did not receive the attention demanded. Since there was almost no one with adequate knowledge of the complex export control regulations at these centers and, at least initially, almost none of the technically knowledgeable scientists and engineers responsible for the development or use of the software had anything more than passing knowledge of the regulations, it is not surprising that it was difficult to obtain a coherent set of responses. Indeed, an earlier Audit Report[9] by the Office of the DoD Inspector General on export control processes at DoD research facilities dated March 2000, examining DoD's implementation of the export control regulations in a broader context, concluded that:

---

[9] Audit Report: Export Licensing at DoD Research Facilities; Report No. D-2000-110, (March 24, 2000), Office of the Inspector General, Department of Defense.

> "DoD research facilities did not have procedures for determining whether a deemed export license was required in conjunction with the disclosure or release of technical data to foreign nationals. In addition, Military Department program officials were not knowledgeable of the term "deemed" or of the licensing requirements for deemed exports."

One can only conclude that, due in part to the complexity of the issues involved in the determination of the export control status of software, it has not been possible to install workable procedures to facilitate the process in the one year elapsed since the problem was identified.

3.3 Examples of DoD Export Control Determination

Although there were many cases decided without adequate knowledge of the relevant regulations, there are a number of examples of quite successful and proper determination of export control status of DoD-developed software. Most of these cases derive from some participant in the process, usually but not always, one of the software scientist/engineer developers who has expended the time to understand the export regulations. In most of these cases, but probably not all, the appropriate issuing authority has concurred with the determination. As this issue continues—and it will—one can expect improvement in the process as the issues become better understood, more participants have moved up the learning curve, and knowledgeable people are identified.

One illuminating example of the difficulties that were encountered in responding to the first call for export control status determination is a documented Navy laboratory-wide case. Also listed are examples of export control determinations of computer codes of selected CHSSI[10] projects that display the range of issues that were encountered in the process. In all there were about 100 CHSSI applications codes in the sample. These include many but not all of the software codes under development by the HPCMP community. The following examples illustrate some cases that led to appropriate status determinations and other cases where the status determinations are questionable.

Laboratory-Wide Example

Starting shortly after the call in February 2001 for the export control status of all HPCMP software, a security officer at one Navy laboratory confronted with the need to determine the export control status of several software projects formally requested guidance on the matter from his supervisor located at another Navy laboratory. The questions asked were (1) should the principal investigators (PIs) responsible for these software products make an export control determination and (2) who should sign for the security concurrence? This request initiated a number of actions including (1) contact with the Navy International Programs Office (NIPO) in the Chief of Naval Operations (CNO) Office, with the response that NIPO had responsibility and that request for guidance should be made to

[10] CHSSI is an application software development program that provides DoD computational scientists and engineers with technical codes that exploit scalable computing systems. The CHSSI applications are selected based on their critical need. These products facilitate a large fraction of the DoD science and technology and developmental test and evaluation computational workload in support of DoD warfighting requirements.

NIPO, and (2) contact for advice with the OSD (Policy), which serves as the OSD FDO, received the response that this is not an OSD issue but a NIPO issue, since the Navy is the better judge of the export control issues of a particular software product. However, based on facility legal counsel advice that government installations are not subject to these export regulations, the originating Navy laboratory security officer advised the PIs not to sign the letters defining export control status on the basis that "some wording on the form was ambiguous and that our scientists were being asked to make an unreasonable determination as to the export control issues." As of the end of August 2001 several of these software export control status determinations had not yet been completed.

Signal/Imaging Processing (SIP) Examples

Four CHSSI program projects, all in the Signal/Image Processing (SIP) CTA are interesting examples of how the export control status determination process proceeded. Two cases, both Air Force projects (AFRL-IF) with the same PI, are SIP-01, RADAR, with four codes under development covering a wide range of the functionality of radar signal processing, and SIP-07, Image Fusion and Signal/Image Processing, which is developing a process to establish a repository of previously developed CHSSI SIP codes and an integrated process to access them. In the short time available for the response, the PI became familiar with both the ITAR and the EAR and had concluded that SIP-01 software was export control exempt. Although he was less certain concerning the status of SIP-07 software it was his belief that it also was export control exempt. When he contacted the local FDO for concurrence and authorization he was told that "all software must be controlled—period." The PI, recognizing that this was in a gray area and desirous of concluding the export control status of all the software, in mid-April, 2001 determined that all the SIP-01 and the SIP-07 software were export controlled. As late as the end of August 2001 the official status for SIP-01 software is listed as "export control exempt—awaiting security office signature," and the status for SIP-07 software is listed as "incomplete."

In the case of SIP-06, Acoustic Analysis Workbench using Windows NT, a Navy project (SSC-SD) developing a problem solving environment to facilitate the analysis of full-spectrum acoustic signatures of undersea objects using a series of filters, the PI felt very strongly that the software should be export control exempt. The PI wanted to share the code with as wide a community as possible to advance the development of the program. Although he felt pressure to declare the code to be export controlled he received concurrence from his supervisor and from the local Public Affairs Office. It is interesting to note that the local security office declined to be involved since the code was not classified. The software status is now officially export control exempt.

SIP-02, Scalable Algorithms for SONAR Beamforming, is a Navy project (NUWC) developing three software codes which perform different beam-forming transformations of hydrophonic time series data. The PI's supervisor believes that all SONAR related codes should be export controlled—and possibly should be controlled even more stringently than export control status requires. The status of the three codes developed in SIP-02 are now export controlled.

Computational Structural Mechanics (CSM) Examples

CTH is a multi-material, large deformation, strong shock wave, solid mechanics parallel computer code developed at Sandia National Laboratory (SNL). This code includes models for multi-phase elastic-viscoplastic, porous, and explosive materials and is used mainly for military purposes. It is used by CSM-03, Scalable Algorithms for Shock Physics, and several other DoD HPCMP user groups. An extensive SNL website is available defining the parameters of the program, its performance, and makes available support documentation. Realistic legitimate dual use of this application is quite small; the oil exploration industry is such a user. SNL, which appears to have a quite well organized process for the export control status determination of the software it develops has declared CTH to be export controlled. The software is licensed to about 250 users, including one from the UK and one from Canada. Except for NT platforms, source code is distributed to all licensees and updated on an 18-month basis. In this case it was only a formality for the CSM-03 group to declare CTH to be export controlled.

ParaDyn is a parallel version of DYNA which is a general purpose, large deformation, contact-impact, Lagrangian-based, finite element, scalable software suite for simulating large-scale practical problems in solid mechanics. It was developed at Lawrence Livermore National Laboratory (LLNL) and used by CSM-02, Large Deformation Finite Element Scalable Software for Structural Dynamic Applications, as well as by several other DoD groups. Parallel and 3D extensions to the code developed by the CSM-02 group and inserted into the distributed software by the LLNL development team, now allow for many problems to be treated at the system rather than at the component level of analysis. This code was determined to be export controlled at LLNL and consequently for DoD the export control status is pre-determined. Run-time code is distributed for most users and identified selected users receive source code. It should be noted that there is a very large set of dual-use problems and a very large community of potential non-defense oriented users of this class of code. Indeed, the original developer of the serial version of the DYNA code at LLNL now is the technical force behind a successful commercial company distributing a number of products including a parallel 3D version of DYNA, called LS-DYNA, with attributes very similar to the ParaDyn code. That product is not export controlled and it should be noted that there are several other vendors offering equivalent functional software. Finally, the LLNL group leader at the time of the decision to declare ParaDyn as export controlled, indicated that the LLNL security personnel involved in the decision did not believe that the availability of a non-export controlled commercial version is a factor in the decision. This is at variance with the ITAR regulations.

An interesting example is ARES, a crack propagation code, being developed in a collaboration between CSM-05, Next Generation Scalable Finite Element Software to Describe Fracture, and a Cal Tech aeronautics and applied mechanics academic group. The current export control status is that the ARES code is not now controlled, but in the third year of the development of the code, the data for the sensitive computations that the group is interested in pursuing will be embedded in the software, thereby making the ARES application package (software and data) export controlled. The academic PI collaborator believes that with the sensitive data removed the software is export control exempt. Furthermore, it is his belief that, if the software is declared export controlled, his group invariably including some foreign students, will no longer be able to participate in further

development. He believes the consequences of that happening will leave the ARES code "obsolete" in a year or two.

Computational Electromagnetics and Acoustics (CEA) Example

XPATCH is a high frequency asymptotic ray tracing code of the "shooting and bouncing rays" type of electromagnetic code being developed for CEA-01, ATR Target and Scene Generation Code. The code is export controlled and is used at over 400 user sites, many of these participating in the HPCMP. Code development is performed by SAIC. There are a number of realistic legitimate dual uses of this type of code including medical imaging and cellular communications. There are other versions of the code available, but there does not appear to be a single stable firm marketing a non export-controlled equivalent product. The XPATCH code is distributed to the many users encrypted on CD-ROM as sensitive modules requiring a software mode lock. Future encrypted distributed versions will require hardware and software keys for a specific platform. The designers of this code plan to have multiple release versions of the code in the future, including a classified version and a non-export controlled version. This approach is an example of how to release dual-purpose code and also control the same code at various levels of sensitivity. This may serve as a model for approaches to the export control issue for a wide range of DoD applications software code.

3.4 Experiences Outside of DoD

Government laboratories in other agencies, especially DOE and NASA, typically with a longer history of involvement with technology transfer programs, appear to have more mature processes in place to deal with export controls. LLNL, which developed ParaDyn, and SNL, developer of the CTH Eulerian shock code, both have systems in place to assist the technical community in the determination of export control issues.

The most interesting example of a well-honed and documented export control mechanism is that of IBM. At IBM there are a multitude of different classes of activities that require export control status definition. In order to stay within legal bounds and preserve its intellectual property rights for its technical data, software and manufacturing processes, IBM has a 200 person organization to facilitate this process worldwide. There are also proprietary web pages available on the IBM intranet to promulgate the necessary information to IBM employees, assist them in the determinations, and expedite the decision process.

Many other large firms, e.g., UNISYS, appear to be less well organized. At the other end of the spectrum the large number of small firms generating interesting new software with only a few employees must deal with a very difficult situation. Typically, they use whatever legal assistance they have available for other purposes to serve as their interface with the DOC and the DOS. Here the experience level in this domain is likely to be very low. The process is usually difficult, painful, time consuming and costly, and likely will conclude with a bad result.

3.5 HPCMP Resource Centers Operational Control of Software and Technical Data

All of the HPCMP resource centers are sensitive to the need to control access to the software and data resident on their systems. Most of the resource centers use the standard UNIX user/group protection and permission procedures, usually along with the Kerberos network authentication protocol, to control access. Other resource centers use the wide-area file system, AES, or similar systems, all of which provide a range of capability approximately the same as the standard UNIX utility.

The standard UNIX utility controls access to any individual file, data or executable software, by specific users or groups of users. Control of these access lists is vested either in the creator user of the files or the center systems administrator. Typically, access to software acquired by or developed by an individual user remains under the control of that user. Access control to more general multi-user software typically remains in the hands of the systems administrator.

These access control mechanisms restrict access to software or data without regard to the specific reason for the restriction. These range from a code being restricted as export controlled, or as labeled NOFORN, to commercially imposed limitations for purchased or licensed software controlled by a list, or on the total number of simultaneous users for a specified program file. It also covers, in the case of owner or user control, data that the owner has chosen to restrict access to the files for any of the above reasons and also any other reason, e.g., to maintain proprietary control of the software, or because the material is still under development.

In all of these cases, there is generally no natural mechanism for distinguishing the reasons why access to a file is restricted. Thus, a code with restricted use developed by a user that is export controlled cannot be distinguished from a second code developed by the same user restricted because the user does not want to distribute it for some other reason. Also, some of the classified resource centers consider that SBU export control issues are not relevant to them because all their users hold national security clearances and all of their software is considered classified. In these cases, even the distinction between classified files and unclassified files (export controlled or export control exempt) is lost.

4. Discussion

4.1 Technical Data and Software Issues

The term technical data as used in the export control regulations includes software. Indeed, software is data, but there is also a class of computer-oriented data that is not properly software, but rather the data that the software (more precisely the process that is controlled by the software) uses to solve a particular problem posed by the software user. Good computer software engineering design[11] typically separates the software (the process) from the data.

This situation provides an important opportunity in the determination of what software to subject to export control. There actually are two relatively independent elements that can be controlled. These are the application program software (the code) defining the process and the data required for executing the software for a particular problem. In some cases, removing sensitive data from an application program package, leaving only a dual-use software application, may be all that is necessary to properly desensitize the program. Denial of the critical data, e.g., physical characteristics of an unusual material, or data resulting from special experimentation, will inhibit solution to the military problem, but the software disseminated without that data may still be very useful for solving civilian problems.

4.2 Dimensions of Export Control

To properly adhere to the intent of the export control statutes with respect to technical data and software there are actually three separate issues, or dimensions, to be resolved. These are: (1) the proper **determination** of the export control status of the technical data or software, (2) the operational **control** of the digital files containing the data and the associated technical literature to support the use of the software and data, and (3) the **dissemination** of the material to foreign nationals.

As discussed earlier in Section 3.5, the HPCMP resource centers take responsibility for the operational control of software and technical data. There are some extensions to the current approaches that are desirable. For the dissemination of information there is a well-defined process in place with the FDOs identified as the office with responsibility for authorizing the transfer of information to foreign nationals. However, as indicated in Section 3.2. of this report there is inadequate understanding of the handling of deemed exports.

The major problem that the HPCMP has encountered in attempting to respond to the directive to focus on the export control of sensitive software has been the lack of definitive

[11] Earlier computer software design frequently did quite the opposite, embedding data into the software modules. Although there are many reasons for exceptions, e.g., performance considerations, the modern approach is to separate the two.

guidance in the determination of the export control status of the technical data and software developed in the program. This situation must be rectified. The primary focus of the remainder of this report is on this issue.

4.3 Some Issues in Export Control Determination

As indicated previously, the export control regulations are convoluted and open to a very wide range of interpretations. In particular, software is a complex item with many attributes making it difficult to define metrics to determine which software should be controlled. Key performance parameters to be considered relative to other similar software include:

- Uniqueness to military applications
- Sophistication of scientific or engineering problems capable of solution
- Level of performance
- Resolution (accuracy) of the computational result
- Ease of use
- Extensibility of the code into new domains
- Breadth of dissemination of equivalent software

Much of the software and associated data in question has legitimate dual-use character, is freely distributed within the larger research community, or is an extension of an already widely distributed code. Sometimes there are available equivalent commercial products. In all these cases, the decision then rests upon the relative effectiveness (in the parameters listed above) of the software under consideration in comparison to other available software. An important discriminating issue is whether or not the code is based upon general scientific, mathematical or engineering principles, or is in the public domain. Alternatively, for code constructed specifically for a military application with no equivalent analogs in civil applications, or code that has significant military or intelligence applicability, the decision is more straightforward.

There are a number of arguments that have been made within the HPCMP community during the recent systematic effort to determine the export status of all software in development or use, that are not appropriate to the export control determination. These include the argument that any code developed by a DoD Laboratory or one of its contractors must be export controlled. Yet another reason used to declare code export controlled is that otherwise, if the code is distributed, it is impossible to guarantee that it will not be further disseminated. Some members of the community have determined that their code is export controlled to more effectively control distribution of code under development or immature code, or out of concern that in the hands of unfamiliar users the application software might give incorrect answers, thereby reflecting on the reputation of the authors. The use of these arguments for declaring software to be export controlled falls outside the spirit of the legislation and the regulations.

4.4 Export Control Determination Process

The lack of a well-defined export control determination process has been a major contribution to the difficulties the HPCMP experienced earlier this year as described in Chapter 3. Similar problems are almost certainly to be encountered when calls for export control status for software are extended more broadly across DoD. The situation for software is quite different from the process involved within the DoD for the determination of the national security classification level of paper documents, where the organizational structure is in place to formally label documents and how documents at various levels of restriction are to be operationally controlled. This mature process has developed over a very long period of time. On the other hand, the export control of software has not yet adequately matured to have established an equivalent organizational structure. Furthermore, the fact that the software code is not prose and is always primarily available as digital data files, complicates the interpretation of its nature by external reviewers. Another major additional complicating factor is the rate of technological change in IT. Software that may be unique one day may rapidly be made obsolete by some new research or commercial product that appears in the marketplace only months later.

Determination of the export regime in which technical data falls is best made by the scientist or engineer responsible for its existence in collaboration with his superior and the cognizant export control agent in the organization. It is imperative that the export control agent be knowledgeable of both the ITAR and the EAR, and has an understanding of the unusual characteristics and special attributes of software, or access to technical support in this regard.

There are processes in place intended to facilitate the status determination of the software under consideration from both DOS and DOC. DOS accepts a Commodity Jurisdiction (CJ) request, which is a free form document used to provide the required information concerning the item (software) under consideration. DOC offers a one page form (Form BXA-748P) used for multiple purposes, including a "classification request." Once submitted, these requests enter a process with little or no feedback to the author(s). Therefore, it is important to submit these forms with detailed and clear descriptions of the software, its use, references to similar software that may serve as precedents, and with a clear understanding of the relevant export control regulations. It is here where the experience of a professional export control expert can be important in describing these aspects of the software and relevant related available software which is pertinent to the decision process. The technical information itself must of course be supplied by the scientist or engineer responsible for the software.

It is very difficult to define a quantitative metric that makes the decision on which software to export control easy. This leaves the final status decision to interpretation of the complex sets of clauses in the export regulations. An important discriminating factor for code specifically constructed for a military application is whether it has equivalent analogs in civil application or has significant military or intelligence applicability. Another important discriminating issue for control is whether or not the code is based upon general scientific, mathematical or engineering principles or is in the public domain.

The distinction between export controlled and export exempt technical data and software is complex and delicate. Data and software should be evaluated in the total context

against the export control regulations. Although there is frequently a large gray area, data in the control regime must be controlled and data in the exempt regime should be exempted.

4.5 Issues of Balance in Export Control

In the R&D arena where most HPC codes are developed and used, there is a natural tension between the demands of science and technology and of national security—a clash of cultures. Good science and technology thrives on sharing information, while good national security often requires limiting access to information. Tensions to be balanced include national and economic security, shared development or refinement opportunities with non-government (e.g., university) participants and intellectual property rights, including publication and commercialization opportunities. An optimal approach should encourage understanding of how to find a balance, taking cognizance of all these issues.

It is useful to understand the effects of export control. Export control improves national security and effects non-proliferation of software code, especially to rogue states. It also guarantees that the official participating community is identified and it inhibits the widespread dissemination of the code. On the other hand, export license exemption broadens participation by the intellectual community to debug, mature, extend the code, and use it for multiple useful ends. Since so many of today's graduate students are non-citizens, only that software that is export control exempt will be able to maintain university participation in continuing to develop and enhance the software. It also enhances dissemination of the code to other legitimate DoD and other government agency potential users.

It is most important to identify that code and the associated data that enables advanced weapons design, performance, capability, maintenance, etc., or supports a more sophisticated warfighter decision process, or command and control capability. Codes and code variants of more general (dual-use) codes written specifically for these purposes and sensitive data sets should be export controlled to the largest extent possible. Dual-use software used to support the warfighter, falls into a separate category. In those cases where such software exceeds the capabilities of equivalent software available in the public domain, it also should be controlled as discussed above. However, it is counterproductive and will lead to a false sense of security to attempt to control dual use software that is widely available in the public domain. Further, such situations may frustrate some in the science and engineering community who then conclude that the process is chaotic and the control efforts are futile, leading to their lack of cooperation.

---

[12] The regulations do not define equivalent. Certainly it is not in the spirit of the regulations to mean identical; i.e., identical code.

5. Findings, Consequences, Approach

5.1 Findings

The information gathered in this study leads to a number of findings summarized in this section.

Finding #1: Both the ITAR and EAR are copious, convoluted, and open to a very wide range of interpretation.

Because of the ubiquitous character of computers in today's world, references to them or to the software that controls how they function appear in many different sections of the export control regulations. In an attempt to minimize repeating definitions, clauses, exception, etc., both the ITAR and the EAR contain many internal cross references. Since the various sections were typically written for different aspects of the problem and probably by different people at different times, frequently there arise apparent inconsistencies, or at least ambiguities, as to how to resolve overlapping regulatory statements. For example, in the USML (Part 121 of the ITAR), which is organized into twenty-one categories of material, in each category there is a similar but not identical clause on computers or software. These all reference basic clauses on technical data and defense articles in Part 125. In some cases, these references appear to be contradictory with the specific USML category exclusion or restriction clause. When applied to general-purpose scientific or engineering software being used for example, in the design of a ballistic missile, these "conflicting" clauses complicate the decision process for determining export control status.

Finding #2: OSD and Service guidance on the export control status determination process and in identification of the office(s) with responsibility is inadequate.

Although each of the Services publishes guidance documents on export control determination, they do so by compiling appropriate extracts from the export control regulations. Any guidance given in association with these extracts tends not to focus adequately on the issues of software. Some informal guidance material[13] is quite good, but it is not authoritative and typically is not widely distributed. While approval authority for the transfer of technical information, including software, and visits to the research laboratories by foreign visitors rests with the FDOs, there appears to be no clear cut designation of authority or POC to assist in the legal and technical interpretations of the regulations for the actual determination of export control status.

[13] For example, see, "Dissemination and Protection Sensitive, Unclassified Information: Everything You Ever Wanted to Know...and More," Briefing by Chuck Chatlynne, Air Force Office of Scientific Research. Available at URL: http://afosr.sciencewise.com/afrinst.htm.

Finding #3: Knowledge of export control regulations and policies by the DoD scientific and engineering community developing or using software varies widely.

Most of the R&D community is focused on their areas of scientific or engineering research activity. They typically have little time and little interest in issues of export control. The likelihood of engaging their cooperation on such a matter rapidly decreases as the demand of their time or the complexity of the issue increases. Consequently, the current state of the export control regulations and the lack of good and clear guidance from OSD and the Services results in relatively few in the R&D community becoming knowledgeable enough about the export regulations to facilitate effective determinations. Those who have spent the time to understand the issues have managed to facilitate meaningful and appropriate export control determinations.

Finding #4: Lack of clearly identified individuals with export control knowledge and designated approval authority leaves software developers without expert assistance to facilitate export control status determinations and to obtain the required approvals.

Although the whole R&D community is sensitive to the national security aspects of the export control regime, in many cases developers of software were unable to locate a local POC to direct them to the appropriate authority. Without expert assistance on the regulatory and policy aspects the export control status determinations may be unreliable. Furthermore, in some cases, because of concern of their personal liability in the case of (even unintended) laxness, there is a tendency to be overly restrictive in the determination process.

Finding #5: There is no generally accepted software development strategy that both advances the research program and addresses export control regulations.

Since most R&D software is developed by the DoD research community, frequently in collaboration with research colleagues at other government centers, corporate research laboratories and academia, it is important to nurture those collaborations to the largest extent possible, without compromising national security. It is important to strike a balance between the security achieved with export control restrictions and the software enhancements achieved with collaboration with members of the larger research community. There are no articulate guidance or policy declarations on this matter.

Finding #6: Although all the resource centers invoke standard operating system or equivalent file access control systems for both data and executable software, there are no clearly defined mechanisms to label restricted files with the type of restriction.

The standard file access control UNIX utility controls access to individual files by specified user or groups of users. Control of the access list is vested either in the user who creates the file or the center systems administrator. Regardless of who places the restriction on access to the file, the reason for limiting access does not accompany the list. Consequently, one cannot distinguish between files that are restricted because they are export controlled, commercial software license limited, or held as proprietary by the user, among other possible reasons.

5.2 Consequences

The complexity of the export control regulations, especially with respect to software, the lack of a well-defined, publicized, and supported process for determining the export status of software, and without explicit assignment of a knowledgeable designated approving authority, sometimes results in software that is determined to be export controlled that should not be, and vice versa. The initial process used by DoD to control software, rather than hardware, to inhibit the growth of technological sophistication on the part of U.S. potential adversaries needs refinement. The process works best when the designated export control authority is adequately knowledgeable of the regulations as they apply to software and technical data, and the software developer/user PI understands the state-of-the-art of equivalent software and the options for export controlling sensitive software and data while simultaneously continuing effective development of the software.

The consequences of a poorly defined process are lost time and effort for DoD and increased workload for the science and engineering community. Furthermore, it potentially allows dissemination of sensitive software to potential national adversaries. On the other hand, the consequences of an overly restrictive stance are the inhibition of the dissemination of useful software technology within DoD, and between its contractors and industry more generally. One of the most serious consequences of unnecessarily inhibiting the dissemination of software technology is the negative effect that it will have on some of the DoD R&D communities' collaborative efforts with the U.S. academic community.

5.3 An Approach to Export Control Determination

It should be accepted that any unclassified material, SBU included, cannot be 100% effectively controlled even by the most stringent export control policy because of the character of software or, more generally, technical data in comparison to physical items. The best a policy can do is to inhibit the release of controlled software to unauthorized parties. Simultaneously, the policy should not unduly inhibit further technical development and appropriate scientific and engineering research collaboration. A good policy will strike a balance between protecting the national security and nurturing R&D. A number of relatively easy actions can be taken to improve the export control determination process in this context. These may be characterized as "process definition" and "product analysis."

Process Definition

Establish a well-defined process for the determination of the export control status of software and technical data. The responsible authority should be explicitly identified and should be knowledgeable of the relevant export control regulations, especially as they apply to technical data. Easy access to technical expertise should be available to this authority when it is required. This authority should be the scientific and engineering community's primary point of contact for export control determinations. The export control determination should result from a detailed analysis of the technical and regulatory issues by the PI (or the PI's supervisor) and the Service export control authority or a local authorized representative.

To facilitate this export control determination process requires developing a clear and concise document defining the process and explaining the various technical facets to be considered in the determination—a cookbook for export control procedures for DoD

software under development or in use. The technical issues should include not only the collection of appropriate clauses from the regulations themselves, but also a discussion of the nuances of interpretation and a list of the secondary issues that may arise. Options as to how best to satisfy both national security concerns and the continuity of R&D should also be included. (See next section on product analysis.) This information should be widely distributed. Web-based approaches to facilitate this information dissemination should be utilized. Also develop a web-based interactive export control status determination decision logic tree to facilitate implementation.

Product Analysis

The very first step in analyzing the appropriateness of export controlling a software product developed in-house is to realistically assess the available software equivalent[14] to the code under consideration in the public domain or for sale by a legitimate commercial firm. Control only that software that enables better solutions either in time or space domains, performs more effectively, is more user friendly, or is more easily extensible than the open alternative software. It is counterproductive to control an application when there is a commercial firm selling an equivalent or better software package in the open market place.

In many cases, the issue of importance in determining the export control status is not the software but the data used with the application software to solve a particular (military focused) problem. In such cases, a more detailed analysis should be considered and an evaluation of several options leading possibly to multiple versions of the application software, some export controlled and some not controlled, may be appropriate.

For any developed application software, consider code and data as separate entities. This is good software engineering practice and in many cases it may uncomplicate the export control decision. Analyze the export control attributes of the code and control that software that meets an appropriate level of sensitivity. Fully release that dual-use software that is not sensitive. For codes that are dual use, but determined to be export controlled, allow for the configuration of a sanitized version of the code that may be considered export control exempt by removing sensitive subroutines or processes (e.g., weapons-based model routines). For codes that are determined to be export control exempt, analyze the associated data sets. If the data is not sensitive then it can be distributed with the code. If some or all of the associated data is sensitive and should be export controlled, then develop two (or more) separate versions of that application, one containing all the associated data, and determined to be export controlled. Other versions, with all sensitive data removed, may be determined to be export control exempt and therefore openly distributed.

---

[14] The regulations do not define equivalent. Certainly it is not in the spirit of the regulations to mean identical; i.e., identical code.

6. Recommendations

Recommendation #1: Ensure that a well-defined export control determination process is in place within the Services and agencies and identify the responsible authority.

The responsible authority for each Service and agency may have representation at the major DoD laboratories and other locations where software is developed and used. These representatives must be knowledgeable of the export control regulations as they apply to technical data and software. They should also be conversant with the range of science and technology spanned by the software under consideration, or have ready access to subject matter experts to assist them when necessary. Where there is no direct representative, some local (security, FDO, STINFO, or public affairs) official should be designated as the POC to direct queries to the responsible export control authority. These POCs should not participate in the export control determination unless they have been explicitly designated as representatives of the export control responsible authority.

Recommendation #2: Develop a clear and concise source book containing the details of the export control determination process, and provide guidance on how to perform the export control determination analysis on any software or technical data item.

The source book should be developed in coordination with the Services and should provide guidance to the implementers of the export control determination, i.e., the export control authority and the software development PIs. It should also provide guidance to the software developers promoting modular development of code and organization of data in order to identify and easily separate the sensitive components from those parts that are not sensitive in cases where that is appropriate. The source book should also provide the nuances of interpretation of the relevant regulatory clauses and the secondary issues that may be relevant in individual cases, helping to guide the participants through what may be a gray area in the export control regulations. Options as to how best to satisfy both national security concerns and the need to foster R&D should also be included. The source book should be widely disseminated and an ongoing training regime in its use should be available.

Recommendation #3: Have export control determinations made by the Service export control authority or authorized representative working directly with the project PI and in conjunction with the PI's management.

The PI or the PI's designated technical experts usually will have the necessary technical information regarding the software item under consideration. The export control authority representative brings an understanding of the export control regulations, especially as it pertains to software and technical data. The export control authority representative should also have some knowledge, or have ready access to technical experts, in the scientific/engineering area of concern. It is their collaborative effort that is likely to assign the most appropriate export control status to the particular software item under consideration

Recommendation #4: Require periodic re-evaluations of the export control status of all controlled software.

Information technology items continue to change at a very high rate. Shortly after an advanced application software module is completed and in use, it may have overwhelming competition from a new yet more advanced product. An appropriate export control status originally determined to be controlled, under these circumstances, may now properly be changed to an exempt status.

Recommendation #5: Require the HPCMP to strengthen procedures for protecting software that is determined to be export controlled.

It is desirable to install more formal procedures for software determined to be export controlled than is currently the practice in some of the shared resource centers. This could serve as a model for other DoD entities developing or using software that is determined to be export controlled. One aspect of such a plan could be the development of a labeling scheme to more uniquely identify the type of restriction (e.g., export controlled, commercial license limitations, user proprietary) of each file.[15] Appendix B suggests a possible organizational scheme.

[15] A labeling scheme need not be complicated, i.e., it need not be integrated into the operating system access control functions. Its primary requirement is that it enables the discovery of the reason a data file is considered restricted.

Appendix A. Contact List

- DoD Users
  - Spiros Antiochos: NRL - DC
  - Robert Bernecky: NUWC - RI
  - Jay Boris; NRL - DC
  - Keith Bromley: SSC - SD
  - Dennis Cottel: SSC - SD
  - Jeff Hughes: AFRL - SN
  - Marvin Kuznitz: NUWC
  - Richard Linderman: AFRL - IF
  - Raju Namburu: ARL
  - Dimitri Papaconstantopoulos: NRL - DC
  - Robert Peterkin: AFRL - DE
  - Zen Pryk: AFRL - IF
  - A. M. Rajendran: ARL
  - Betsy Rice: ARL

- DoD (HPC) Management
  - Steve Adamec: NAVO
  - Chuck Chatlynne: AFOSR
  - Tom Hitchcock: OUSD(AT&L)
  - Charles Nietubicz: ARL
  - Leslie Perkins: HPCMP
  - Virginia Ross: AFRL - IF
  - Randy Shumaker: NRL - DC

- DoD Export Control Focus
  - Kelly Cagwin: AFRL - IF/STINFO
  - Victoria Cox: ODUSD(S&T) - BR/International Plans & Programs

- Lothar Harris: US XPORTS - OUSD (Policy)
- Russ Miller: AFRL - IF /FDO
- Oksana Nesterczuk: DTRA
- Linda Randall: DTRA
- Jim Sell: DTRA
- Jim Woody: DTRA

- Other Government Agencies/Contractors
  - Sam Cipino: NASA - Langley
  - Dave Cooper: LLNL
  - Dona Crawford: SNL
  - Eugene Hertel: SNL
  - Jim Lewis: DOC (formerly)
  - Steward Pendleton: NASA - Langley
  - Peter Raboin: LLNL
  - Tammy Sanchez: SNL
  - Steve Sultemeier: SNL
  - Chad Twitchwell: SNL
  - Ron Williams: SNL

- Commercial Firms
  - AeroSoft, Inc.
  - Boeing Aircraft Co.
  - Company Coalition of Responsible Exports (CCRE)
  - IBM
  - Livermore Software Technology Corp. (LSTC)
  - MPI Software Technology, Inc.
  - UNISYS

- Academia
  - Michael Ortiz: Cal Tech
  - Jim Pool: Cal Tech

Appendix B. Technical Data Labeling Proposal

- Operationally there are a number of different regimes defining the use and distribution of technical data (both software codes and data). There is merit in categorizing data falling into these regimes. These regimes which are not exclusive include:

- Determined to be export controlled
- Determined to be export license exempt
- Export control status not yet determined
- Proprietary data
- Data under (limited) license
- Limited use or distribution under authority of developer/user/sponsor
- Use and distribution limited to U.S. Government and their contractors
- Use and distribution unlimited
- Code under development
  - Use and distribution unlimited
  - Use and distribution limited
  - Export status presumed controlled
  - Export status presumed license exception

For example, to properly characterize the various types of control regimes for SBU technical data define and implement a technical data-labeling scheme:

- Export controlled under ITAR
- Export controlled under EAR
- Export license exception — formally determined
- Export status not yet determined
- Code under development
- Distribution controlled by authority of user or developer
- Proprietary data
- Data under license
- Use and distribution limited to U.S. Government and its contractors
- Use and distribution unlimited

Appendix C. Acronyms

AECA	Arms Export Control Act
AFOSR	Air Force Office of Scientific Research
AFRL	Air Force Research Laboratory
ARL	Army Research Laboratory
BXA	Bureau of Export Administration, Department of Commerce
CCL	Commerce Control List, 15 CFR 799
CEA	Computational Electromagnetics and Acoustics
CFR	Code of Federal Regulations
CHSSI	Common High Performance Computing Software Support Initiative
CJ	Commodity Jurisdiction
CNO	Chief of Naval Operations
CSM	Computational Structural Mechanics
CTA	Computational Technical Area
CTP	Composite Theoretical Performance
DDR&E	Director of Defense Research and Engineering
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DTRA	Defense Threat Reduction Agency
DUSD(S&T)	Deputy Under Secretary of Defense (Science & Technology)
EAA	Export Administration Act of 1979
EAR	Export Administration Regulations, 15 CFR 768.799
FDO	Foreign Disclosure Officer
HPC	High Performance Computing
HPCMP	High Performance Computer Modernization Program
IDA	Institute for Defense Analyses
IT	Information Technology
ITAR	International Traffic in Arms Regulations, 22 CFR 120-130
LLNL	Lawrence Livermore National Laboratory
MSRC	Major Shared Resource Center

NASA	National Aeronautics and Space Agency
NAVO	Naval Oceanographic Office
NIPO	Navy International Programs Office
NOFORN	No Foreign
NRL	Naval Research Laboratory
NUWC	Naval Undersea Warfare Center
ODTC	Office of Defense Trade Controls
OSD	Office of the Secretary of Defense
PDUSD(AT&L)	Principal Deputy Under Secretary of Defense (Acquisition, Technology & Logistics)
PI	Principal Investigator
POC	Point of Contact
R&D	Research and Development
SBU	Sensitive but Unclassified
SIP	Signal/Image Processing
SNL	Sandia National Laboratory
SPAWAR	Space & Naval Warfare Systems Command
SSC	SPAWAR Systems Center
STINFO	Science and Technology Information Officer
USD (AT&L)	Under Secretary of Defense (Acquisition, Technology & Logistics)
USML	United States Munitions List

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2001	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE
Evaluation of DoD Policies for the Release and Distribution of Software

5. FUNDING NO.S
DASW01-98-C-0067
Task Order AK-5-1968

6. AUTHOR(S)
Alfred E. Brenner

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria, VA 22311-1772

8. PERFORMING ORGANIZATION REPORT NO.
IDA Paper P-3652

SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DUSD(S&T)
Rosslyn Plaza North, Suite 9030
1777 North Kent Street
Arlington, VA 22209

10. SPONSORING/MONITORING AGENCY REPORT NO.

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, unlimited distribution: 03 January 2002.

12b. DISTRIBUTION CODE
2A

13. ABSTRACT (Maximum 200 words)
Advances in information technology have limited the effectiveness of export control policies on high performance computer hardware. A study by the Deputy Under Secretary of Defense (Science and Technology) (DUSD(S&T)) concluded that an alternative, more effective, mechanism is to control software that is considered to be sensitive. The process for software export control is much less well-developed and understood than the process for hardware. This document summarizes the relevant parts of export control legislation, analyzes the current DoD processes and policies related to the release and distribution of software, identifies the important issues and provides recommendations to assist in software export control determinations and processes.

14. SUBJECT TERMS
Software Control Policy, Export Control Laws, Export Control Legislation, Export Administration Act (EAA), Arms Export Control Act (AECA), International Traffic In Arms Regulation (ITAR), Export Administration Regulation (EAR).

15. NO. OF PAGES
52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL